UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,761	08/31/2001	Robert L. Alldredge	AL0831	2748

26092 7590 09/25/2003

KYLE W. ROST
5490 AUTUMN CT.
GREENWOOD VILLAGE, CO 80111

EXAMINER
CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/25/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/944,761	ALLDREDGE, ROBERT L.	
	Examiner	Art Unit	
	Paul E. Callahan	2134	

-- The MAILING DATE of this communication appears on the c ver sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *31 August 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-7,9-21 and 23-38* is/are rejected.

7)☐ Claim(s) *8 and 22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-38 are pending in this application and have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 7, 9, 11, 23, 25, and 31, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 7, the claim contains the language: "...providing user initiated and user terminated connections to said user." The meaning of the phrase is not clear.

As per claim 9, the claim contains the language: "...that is the number of bits of said communication..." The meaning of the phrase is unclear.

As per claim 11, it is not clear what the applicant contemplates when a service is provided to a user where the service comprises: "goods."

As per claim 23, it is unclear what is meant by "anonymous Internet access." Claim 24 is dependent on claim 23 and is rejected on this basis as well.

As per claim 25, it is unclear what the Applicant means by anonymous e-mail.

As per claim 31, it is unclear what is meant by "preselected data." Claims 32 and 33 are dependent on claim 31 and are rejected on this basis as well.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 10-14, 16-18, 20, 21, and 26, are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Kravitz, (US 6,029,150).

As per claims 1 and 14, Kravitz teaches a method for conducting private secure electronic commerce (abstract) comprising the steps of: providing first and second sequences of encryption key material with said first sequence being suited for decrypting a message that has been encrypted using said second sequence and said second sequence being suited for decrypting a message that has been encrypted using said first sequence (col. 8 lines 20-35), associating a value parameter with said first sequence (col. 7 lines 45-55), providing said first sequence to an anonymous user in exchange for a payment (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67), providing encrypted data communications to said user until said value parameter is exhausted (col. 28 lines 35-30, col. 30 lines 40-47, col. 31 lines 25-30), and adjusting said value parameter in response to said step of providing encrypted data communications (col. 28 lines 35-30, col. 30 lines 40-47, col. 31 lines 25-30).

As per claim 10, Kravitz teaches the method as set forth in Claim 1 wherein said step of providing encrypted data communications includes the substeps of: receiving a message

encrypted by use of said first sequence from said user (col. 27 lines 35-55) , decrypting at least a portion of said message by use of said second sequence (col. 27 lines 35-55), and providing a service to said user in response to said message, and adjusting said value parameter in response to providing said service (col. 30 lines 40-47).

As per claim 11, Kravitz teaches a service is chosen from the group of information, software, goods, communication and calculation (abstract).

As per claim 12, Kravitz teaches the step of providing anonymous (encrypted communications) network access to said user (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67).

As per claim 13, Kravitz teaches the step of providing encrypted application (financial transactions) services to said user (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67).

As per claim 16, Kravitz teaches a method for conducting private secure electronic commerce comprising the steps of: providing first and second sequences of encryption key material with said first sequence being suited for decrypting data that has been encrypted using said second sequence and said second sequence being suited for decrypting a data that has been encrypted using said first sequence (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67), associating a value parameter with said first sequence (col. 31 lines 25-30), providing said first sequence to an anonymous user in exchange for a monetary payment proportional to said value parameter (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67), providing encrypted application

services to said user, providing anonymous network access to said user, adjusting said value parameter in response to said steps of providing encrypted application services and providing anonymous network access (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67), and ceasing said providing encrypted application services and said providing anonymous network access when said value parameter is exhausted (col. 30 lines 40-47, col. 31 lines 25-30, col. 7 lines 10-67).

As per claim 17 Kravitz teaches a method for conducting private secure electronic commerce comprising the steps of: providing a first server, providing to an anonymous first user, in exchange for a payment, a first sequence of encryption key material, an identifier associated with said first sequence, connection instructions for connecting to said server, and encryption instructions for encrypting and decrypting data using said first sequence (col. 22 lines 50-67, col. 23 lines1-17), providing to said server said identifier and a second sequence of encryption key material suitable for decrypting data that is encrypted with said first sequence and for encrypting data that can be decrypted with said first sequence, and providing encrypted data communications between said first user and said first server (col. 32 lines 35-50).

As per claim 18, Kravitz teaches the method as set forth in Claim 17 wherein said step of providing encrypted data communications includes the substeps of: establishing a user initiated connection by said first user connecting to said first server by using said connection instructions, receiving said identifier from said first user at said first server, selecting said second sequence in response to receiving said identifier, receiving, at said first server, from said first user, encrypted

user data that said first user encrypted by using said first sequence and said encryption instructions, decrypting at least a portion of said encrypted user data by using said second sequence, encrypting server data by using said second sequence, and transmitting from said first server, to said first user, said encrypted server data (col. 32 lines 35-50).

As per claim 20, Kravitz teaches the method as set forth in Claim 17 further comprising the steps of: establishing a first user account accessible to said first server with said first user account including said identifier and a first user value parameter that is proportional to said payment (col. 22 lines 50-67, col. 23 lines 1-30), and adjusting said value parameter in response to said step of providing encrypted data communications (col. 30 lines 40-50, col. 31 lines 25-35).

As per claim 21, Kravitz teaches the method as set forth in Claim 20 wherein: said first server is an application service provider, said step of providing encrypted data communications includes said first server providing applications services to said first user (abstract, financial services, col. 32 lines 35-50), and said step of adjusting includes adjusting said first user value parameter response to said providing applications services (col. 31 lines 25-35).

As per claim 26, Kravitz teaches the method as set forth in Claim 17 wherein said step of providing to an anonymous first user includes providing a portable data storage device suitable for access by a data processing device to said first user (col. 4 lines 45-67), said storage device including said first sequence of encryption key material and said identifier as stored data, and

said connection instructions and said encryption instructions as executable software col. 22 lines 50-67, col. 23 lines 1-20).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-6, 15, and 19, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kravitz as applied to claim 1 above, in view of Shefi (US 6,445,794) and Official Notice as detailed below.

As per claim 2, Kravitz does not teach the method as set forth in Claim 1 wherein said first and second sequences are identical one-time pads. However Shefi does teach this (col. 19 lines 5-10) Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature of Shefi into the system of Kravitz. It would have been desirable to do so based on a motive to combine these references that is found for example in Kravitz, col. 6 lines 35-50, where the need for low processing cost in smart card communications is discussed. A one-time pad approach does provide a lower cost alternative than most other cryptosystems owing to its lower computational requirements.

As per claim 3, Shefi teaches the use of a one time pad as noted supra, and Kravitz teaches the step of adjusting that includes adjusting said value parameter in response to utilization of said first sequence such that when said one time pad is exhausted, said value parameter is exhausted (col. 28 lines 35-30, col. 30 lines 40-47, col. 31 lines 25-30).

As per claim 4, neither Kravitz nor Shefi teaches said first sequence and said second sequence each include an identical plurality of sequentially arranged session keys. However official Notice may be taken of the fact that "one-time-pad" cryptosystems are typically comprised of a plurality of sequentially arranged session keys. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Kravitz. An indication of the desirability to do so is found for example in Kravitz, col. 6 lines 35-50, where the need for low processing cost in smart card communications is discussed. A one time pad approach with a plurality of sequentially arranged session keys does provide a lower cost alternative than most other cryptosystems owing to its lower computational requirements.

As per claim 5, Kravitz teaches a step of adjusting that includes adjusting said value parameter in response to utilization of said session keys of said first sequence such that when said plurality of session keys is exhausted, said value parameter is exhausted (col. 28 lines 35-30, col. 30 lines 40-47, col. 31 lines 25-30).

As per claim 6, Kravitz does not teach a step of providing encrypted data communications includes providing user initiated and user terminated connections to said user with said user

utilizing a new session key from said plurality of session keys of said first sequence each time said user initiates a said connection. However Shefi does teach this in col. 5 lines 40-55. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Kravitz. An indication of the desirability to do so is found for example in Kravitz, col. 6 lines 35-50, where the need for low processing cost in smart card communications is discussed. A one time pad approach with a plurality of sequentially arranged session keys does provide a lower cost alternative than most other cryptosystems owing to its lower computational requirements.

As per claim 15, Shefi teaches providing identical one time pad first and second sequences of encryption key material as noted supra, Kravitz teaches providing said first sequence to an anonymous user in exchange for a payment (col. 12 lines 34-45, col. 18 lines 55-60, col. 22 lines 50-67), receiving a message encrypted by use of said first sequence from said user, decrypting at least a portion of said message by use of said second sequence, generating a response to said user (col. 32 lines 35-47), encrypting said response by use of said second sequence into an encrypted response (col. 23 lines 12-17, col. 30 lines 25-50),sending said encrypted response to said user, and ceasing said sending and receiving when said first and second sequences have been completely used once (col. 30 lines 40-47, col. 31 lines 25-30, col. 7 lines 10-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Shefi into the system of Kravitz. An indication of the desirability to do so is found for example in Kravitz, col. 6 lines 35-50, where the need for low processing cost in smart card communications is discussed. A one time pad approach with a plurality of

sequentially arranged session keys does provide a lower cost alternative than most other cryptosystems owing to its lower computational requirements

As per claim 19, The combination of Shefi and Kravitz does not teach the method as set forth in Claim 18 further comprising the steps of: providing third and fourth sequences of encryption key material with said third sequence being suited for decrypting a message that has been encrypted using said fourth sequence and said fourth sequence being suited for decrypting a message that has been encrypted using said third sequence, providing said third sequence to said first server, providing said fourth sequence to a second server, after said step of decrypting at least a portion of said encrypted user data, encrypting said user data by using said third sequence and then transmitting, from said first server, to said second server, said encrypted user data, and prior to said step of encrypting server data, receiving, at said first server, from said second server, encrypted server data that was encrypted by using said fourth sequence, and decrypting said encrypted server data by using said third sequence. However official Notice may be taken that the use of third and forth sequences in this manner is a characteristic of "one-time-pad" cryptosystems. Therefore it would have been obvious to one of ordinary skill in the art to have incorporated this feature into the system of Kravitz and Shefi, an indication of the desirability to do so is found for example in Kravitz, col. 6 lines 35-50, where the need for low processing cost in smart card communications is discussed. A one time pad approach with a plurality of sequentially arranged session keys does provide a lower cost alternative than most other cryptosystems owing to its lower computational requirements

8. As per claims 27-38, these claims represent the apparatus carrying out the method of claims, 1, 15-17, 27, and 34, and therefore are rejected on the same basis as those claims.

Allowable Subject Matter

9. Claims 8 and 22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. Claims 7, 9, and 23-25 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

9/22/03

Paul Callahan
9/22/03